附件 1

“网络空间安全治理”重点专项
2024年度项目申报指南

为落实“十四五”期间国家科技创新有关部署安排，组织实施好“网络空间安全治理”重点专项，根据本重点专项实施方案部署，现发布 2024 年度项目申报指南。

项目坚持服务国家需求，坚持应用目标导向，聚焦国家和行业网络安全重大风险，解决国家网络安全重大技术问题。建立责任部门机制，每个项目确定一个责任部门，一般为项目需求部门。责任部门参与项目实施、中期检查、阶段性评估、“里程碑”节点考核、绩效评价等工作。

本次启动 8 项指南任务，安排国拨经费 4000 万元左右。其中，部署 3 个一般项目；围绕关键信息基础设施安全防护等重点领域，部署 5 个青年科学家项目，每个项目安排国拨经费不超过 200 万元。申报项目的研究内容必须涵盖指南所列的全部研究内容和考核指标，项目以应用为导向设置考核指标，以应用型指标为主，原则上不设置论文指标。除特殊说明外，每个指南支持项目数为 1 项，实施周期不超过 3 年。

一般项目配套经费与国拨经费比例不低于 1:1，项目下设课题数不超过 5 个，项目参与单位总数不超过 5 家，项目

设 1 名项目负责人，项目中每个课题设 1 名课题负责人。

青年科学家项目不再下设课题，项目参与单位总数不超过 2 家，项目骨干人数不超过 5 人。提供研究与验证环境的单位不得申报该指南方向。青年科学家项目负责人应为 1984 年 1 月 1 日以后出生，原则上团队其他参与人员年龄要求同上。

具体项目申报指南如下：

1.基于公网密文流量特征的攻击行为检测分析与追踪技术

研究内容：针对公网中现有检测技术手段难以高效检测密文流量的问题，研究国内公网环境下全流量加密攻击特征提取技术，提取网络流量数据包序列、URL模式、证书指纹、密钥协商等要素特征，构建加密攻击行为特征库，形成SSL/TLS、SSH、RDP等标准加密协议识别分析能力；研究基于常规协议进行隐蔽通信的行为识别技术，针对DNS、ICMP、HTTP等非加密协议开展隐蔽隧道威胁监测识别，发现隐蔽通信流量中的恶意软件及APT组织通信行为；研究密文流量中APT攻击行为检测分析技术，基于加密流量多维度特征识别公网典型APT通信流量中攻击组织、攻击手法、攻击工具等。

考核指标：研制公网加密流量攻击行为识别及特征提取检测设备，支持识别 TLS、SSL、SSH 等标准加密协议，支

持 50 种以上流量要素特征检测、150 种以上攻击链信息检测识别，单台设备（64 核、512G 内存）流量处理能力不低于 20Gbps，在不少于 5 个互联网省级出入口进行部署应用；识别近 3 年隐蔽通信活跃恶意软件家族不低于 100 种，包括但不限于 ColbaltStrike、FastRDP、hydra 等；研制公网加密流量和隐蔽通信监测识别系统，与加密流量攻击识别及特征提取检测设备形成联动检测能力，识别国家背景的 APT 组织不少于 30 个。

有关说明： 责任部门为工业和信息化部。项目承担单位遴选方式为揭榜挂帅。

2.抗量子计算密码迁移关键技术

研究内容： 针对量子计算快速发展给经典密码带来的安全威胁，研究我国商用密码领域自主可控抗量子计算密码迁移关键技术，提出抗量子计算密码迁移总体技术方案；设计抗量子计算密码协议方案和现用密码协议抗量子计算改造方案；研究抗量子计算密码软硬件实现关键技术，研制抗量子计算密码芯片、密码机和加密网关设备；基于国家电子认证信任体系，设计我国抗量子计算电子认证体系技术方案；研究信息系统量子计算条件下密码安全脆弱性检测技术，研制抗量子计算关键密码产品迁移检测验证平台，在关键信息基础设施等领域进行示范应用。

考核指标： 提出我国商用密码领域抗量子计算密码迁移

总体技术方案，支持我国自主量子安全强度达128比特的公钥和分组算法；提出至少2种抗量子计算的网络层密码协议方案和传输层密码协议方案，提出TLS、IPSec等至少2种密码协议的抗量子计算改造方案，量子安全强度均达128比特，研制配套密码协议实现库；研制1款服务端密码芯片和2款终端密码芯片，签名性能分别达到1万次/秒和50次/秒，服务端芯片密码功能可重构；研制2款密码机、2款TLS网关、2款IPSec网关，加密性能达1Gbps；研制1套抗量子计算PKI系统，实现10家运营CA机构接入验证；研制1套数字证书跨域服务系统，在2个应用领域进行验证；研制2款信息系统抗量子计算脆弱性识别工具，支持10种主流密码算法的自动化识别；研制1套抗量子计算关键密码产品迁移适配检测平台，完成5款密码产品适配检测。

有关说明：责任部门为国家密码局。项目承担单位遴选方式为揭榜挂帅。

3.基于标签标识的网络数据治理关键技术研究

研究内容：针对网络数据治理中存在的数据流通追溯难、数据类型甄别难、处理合规验证难等问题，研究网络数据标签标识技术机理与运行机制，提出面向网络数据治理的标签标识标准体系与技术架构；研究多源异构数据标签标识智能化生成与可靠传输技术，实现对海量数据资源多维特征与安全属性的快速标记，构建基于网络传输成功率概率与冗

余传输可靠性模型；研究数据传输一致性校验技术，实现对标识流量数据内容的安全性核查；研究基于异构算力模型的高性能标识流量识别与校验技术，实现大规模流量数据标签标识自动化验标、脱标与数据管理；研发基于标签标识的数据流动合规检测系统，面向典型场景开展服务网络数据治理的技术能力验证。

考核指标：提交网络数据标签标识技术标准草案不少于1项，形成网络数据标签标识运行技术架构方案不少于1套；完成不低于3个重点行业领域、200种重要数据标签标识生成模型，数据标识自动化识别准确率不低于90%，10Gbps流量条件下打标延时不高于100ms，整体标签标识传输成功率大于98%；标识流量数据内容核查成功率不低于95%；单DPU卡数据标签识别流量处理达到50Gbps，单DPU卡的HTTPS加密流量查验1万条规则匹配能力达到10Gbps；研发基于标签标识的数据流动合规检测原型系统1套，典型场景下数据流动合规检测准确率不低于85%，查全率不低于80%。

有关说明：责任部门为中央网信办。项目承担单位遴选方式为揭榜挂帅。

4.面向城市轨道交通系统的网络安全智能防御关键技术（青年科学家项目）

研究内容：针对传统的安全防护手段已无法应对日益复

杂的城市轨道网络安全环境的问题，研究城轨工控系统安全风险监测方法，实现对工控网络威胁的快速与精准识别；研究网络安全智能防御方法，实现对工控网络的主动安全防护；研究异构数据的统一分析和异构设备的集中管控方法，实现兼容多类异构网络安全设备的协同防御。

考核指标：在不基于特征更新情况下，实现攻击识别准确率大于98%；具备网络攻击威胁主动识别和封堵识别一体化能力，自动阻断响应时间≤1秒；具备不少于5类安全设备接入和集中管理能力；支持透明桥接、旁路、双机等多种部署模式；具备有线网络、USB两种形式非法接入自动报警能力，以及恶意连接外部网络的处置能力；在轨道交通业务环境下进行验证。

有关说明：责任部门为交通运输部。南瑞轨道交通技术有限公司提供研究与验证环境。项目承担单位遴选方式为公开申请。

5.大型枢纽通航关基设施跨域联动防御关键技术（青年科学家项目）

研究内容：研究脆弱性关键分析技术，实现对通航枢纽船闸、升船机等设施间的威胁识别；研究基于威胁跨域传播及协同攻击特征的防御技术，实现枢纽通航业务相关的工控设备及基础设施、运行与航运调度系统间的联动防护机制；实现大型枢纽通航关基设施跨域联动防护原型系统的研发。

考核指标：已知威胁检测准确率大于 90%，具备对未知威胁的识别能力；安全事件类型评估时间小于 10 分钟，针对攻击的设施联动响应时间小于 10 分钟；研发 1 套大型枢纽通航关基设施跨域联动防护原型系统，在三峡枢纽通航业务环境下进行技术验证。

有关说明：责任部门为交通运输部。宜昌三峡通航工程技术有限公司提供研究与验证环境。项目承担单位遴选方式为公开申请。

6.自动化集装箱码头异构网络安全防护技术与应用（青年科学家项目）

研究内容：研究动静结合的固件漏洞检测技术，构建港口设备工控固件安全增强设计方法；研究基于漏洞特征的风险评估和实时入侵检测防御技术，实现攻击行为感知与处置；研发自动化集装箱码头工控设备安全检测与防护原型系统，具备自动精确的漏洞检测、入侵识别、攻击预警等能力。

考核指标：支持在10种以上设备安全漏洞检测，获得不少于30个CNVD原创漏洞编号，其中高危漏洞不少于15个；提出港口设备工控固件安全增强设计方法1套，覆盖100种以上漏洞威胁模型；自动化集装箱码头工控网络入侵检测准确率不低于95%，响应告警时间≤10秒；原型系统在年吞吐量超300万标准箱单体自动化集装箱码头进行技术验证。

有关说明：责任部门为交通运输部。上海港罗东集装箱

码头有限公司提供研究与验证环境。项目承担单位遴选方式为公开申请。

7.面向列控系统的网络安全建模与加密车地通信技术（青年科学家项目）

研究内容：面向列控系统网络安全威胁分析和安全防护需求，研究针对列控系统的网络安全建模与分析理论，构建紧密结合列控系统业务特性的网络安全分析模型，为列控系统网络安全防护奠定理论基础；研究基于国产密码的列控系统车地通信技术，实现高速运动和复杂环境下基于双模双通道的高可靠列控车地通信技术，支持国产密码实时加解密，保障列控数据高效安全传输。

考核指标：提出针对列控系统的网络安全分析模型、基于国产密码的列控系统车地通信技术；研制基于国产密码的高可靠车地通信测试原型系统，实现基于双模双通道的高可靠列控车地通信，端到端传输时延不超过200ms，支持SM2、SM3、SM4等国家商用密码算法，SM4加解密速率不低于100Mbps；在铁路列车运行控制系统中开展技术应用验证。

有关说明：责任部门为国家铁路局。研究与验证环境由国家铁路局组织协调有关单位提供。项目承担单位遴选方式为公开申请。

8.面向水利行业大模型的数据安全训练技术（青年科学家项目）

研究内容：面向水利行业水利工程信息、水旱灾害防御、水文监测、水资源等重要数据的安全共享和行业大模型安全训练的需求，研究水利行业大模型的数据安全训练机制，突破大模型隐私安全训练理论，降低水利行业大模型训练与微调阶段的重要数据安全风险；研究面向水利行业大模型精确训练的安全通信优化方法，在不明显损失模型精度的同时实现模型参数的安全交互与动态调整，确保重要数据在通信过程中的安全；研发面向水利行业大模型的数据安全训练原型系统，并开展技术验证，支撑水利行业重要数据的安全共享共用。

考核指标：提出面向水利行业大模型的数据安全训练机制、面向大模型精确训练的安全通信优化方法；研发面向水利行业大模型的数据安全训练原型系统，实现水利行业大模型训练过程中重要数据不出安全域，相比已有联邦学习等分布式模型参数高效微调方法，计算开销增加不超过5%，模型精度损失不超过5%，可抵抗梯度反演、数据投毒、后门攻击、模型内存泄漏等不少于4种攻击类型，水利重要数据反推成功率不超过2%；在不少于1个大型水利枢纽工程进行技术应用验证。

有关说明：责任部门为水利部。水利部小浪底水利枢纽管理中心提供研究与验证环境。项目承担单位遴选方式为公开申请。